

1

PATENT APPLICATION
DOCKET NO. 0100.0001280

In the United States Patent and Trademark Office

5

FILING OF A UNITED STATES PATENT APPLICATION

10

**METHOD AND APPARATUS FOR MAINTAINING SECURE AND
NONSECURE DATA IN A SHARED MEMORY SYSTEM**

Inventors:

Allen J.C. Porter 19 Bowman Way Thoruhill, Ontario, Canada	Chun Wang 735 Don Mills Road #105 Toronto, Ontario, Canada
Kevork Kechichian 135 Briarwood Road Unionville, Ontario, Canada	Gabriel Varga 48 Cynthia Read Toronto, Ontario, Canada
David Strasser 35 Yorkview Drive North York, Ontario, Canada	

15

Attorney of Record
Christopher J. Reckamp
Registration No. 34,414
P.O. Box 06229
Wacker Drive
Chicago, Illinois 60606-0229
Phone (312) 939-9800
Fax (312) 939-9828

20

Express Mail Label No EL 707797155US

Date of Deposit: 5/7/01
I hereby certify that this paper is being deposited with the
U.S. Postal Service "Express Mail Post Office to
Addresses" service under 37 C.F.R. Section 1.10 on the
'Date of Deposit', indicated above, and is addressed to the
Commissioner of Patents and Trademarks, Washington,
D.C. 20231.

Name of Depositor Rosalie Swanson
(print or type)

Signature

Rosalie Swanson

METHOD AND APPARATUS FOR MAINTAINING
SECURE AND NONSECURE DATA IN A SHARED MEMORY SYSTEM

5

Field Of The Invention

10 The invention relates generally to providing data security in a shared memory system and more particularly to maintaining secure and non-secure data in a shared memory system.

Background Of The Invention

15 Many systems contain a data storage device that can be accessed by several processing devices. For example, a graphics processor and a host processor within a computer system may access a shared portion of a memory. Another example is a digital television system, in which a graphics processor (e.g., a graphics chip) shares many system resources with a central processing unit on a processor chip. Typically, various processes executing on the various processors throughout a system can read and write to memory throughout the system. For example, the central processing unit may execute a 20 spreadsheet or other software application that writes graphics images to a monitor, while a 3D graphics rendering engine writes 3D (three-dimensional) graphics images to the same monitor. Accordingly, both processors access information in a frame buffer such as VRAM (video random access memory), SDRAM or any other suitable memory used by the graphics processor.

25

30 A digital television system may be designed to receive a packetized video stream that is both encrypted (e.g., using a copy protection key or other encryption key) and compressed (e.g., using an MPEG encoder). The digital television system may include a decryption module that decrypts the received video stream to generate a compressed decrypted representation of the video stream. The compressed decrypted representation may be used directly, for example to update the VRAM, or it may be uncompressed to provide full images to the VRAM. Typically, the graphics processor stores the

compressed decrypted representation within the VRAM. The compressed decrypted representation of the video stream is then uncompressed to generate an uncompressed decrypted representation of the video stream that is used by the graphics processor to provide images to the monitor.

5

Unfortunately, a compressed decrypted representation of the video stream can be a very attractive target for illicit copying, since it can easily be copied onto another media such as networked storage or a removable medium such as a hard disk, CD-ROM, or DVD and transferred to another digital television system for viewing. The encrypted 10 video stream is a less attractive target for illicit copying since it is only useable by persons having access to a corresponding decryption key. The decrypted uncompressed video stream is likewise a less attractive target for illicit copying since it is so large and may require an inconveniently large amount of storage space.

15

When the graphics processor performs no function other than the decryption and decompression of encrypted, compressed video streams, the problem may be addressed simply by concealing the VRAM within the graphics processor. However, when the graphics processor resides within a digital television system, other processors typically have access to the VRAM. For example, processes executing on a central host 20 processing unit may read data from the VRAM over a user accessible bus such as a PCI (peripheral component interconnect) bus to which both the graphics processor and the central processing unit are coupled.

25

Consequently, a need has arisen for a method and apparatus for securing data in shared memory systems.

Brief Description Of The Drawings

FIG. 1 shows a block diagram of a portion of a digital television system, in accordance with a well-known design.

30

FIG. 2 shows a block diagram of a portion of a digital television system, in accordance with one embodiment of the present invention.

FIG. 3 shows a block diagram of a portion of a digital television system employing an addressed based security technique in accordance with one embodiment of the present invention.

5 FIG. 4 shows a flowchart of a process of accessing data on a graphics processor, in accordance with one embodiment of the present invention.

Detailed Description Of a Preferred Embodiment of The Invention

10 FIG. 1 shows a block diagram of a portion of a digital television system 10, in accordance with a well-known design. The digital television system 10 is used to play video and multimedia content that is received from an originator of the video and multimedia content via a transmission medium. The video and multimedia content may be compressed and encrypted, and may be transmitted to the digital television system via 15 coaxial cables (i.e., cable television), radio-frequency transmissions, satellite transmissions, streaming video transmission over the Internet, or from a CD-ROM, DVD, or hard drive.

20 The digital television system 10 of FIG. 1 is, for example, coupled to receive video and multimedia content via a cable network. The digital television system 10 has a conditional access data provider such as a POD module 16 or other suitable source that is coupled to a head end 12 via an NIU 14 (network interface unit) that receives a radio-frequency transmission from the head end 12 via the cable network. The radio-frequency transmission includes several compressed, encrypted video streams, as well as some 25 “overhead” information that is used by the digital television system to interpret the radio-frequency transmissions.

30 The NIU 14 provides a TS (transport stream) to the POD (point of deployment) module 16. The TS is encrypted with a “conditional access” encryption protocol, which may be referred to as a “scrambling” protocol. In the example shown in FIG. 1, the

conditional access encryption protocol is proprietary, although publicly available conditional access encryption protocols may be used.

5 The POD module 16 performs an inverse conditional access algorithm to decrypt or “descramble” the transport stream to generate an unencrypted, compressed representation of the video streams.

10 The POD module 16 then encrypts the unencrypted, transport stream containing compressed representation of the video streams using an encryption scheme such as a DES data encryption standard ECB electronic code book. In other words, the POD module 16 performs data encryption using an ECB mode of DES. Because the transport stream is encrypted, accessing the video streams at this point does not allow an illicit copier to obtain a marketable version of the video streams.

15 The POD module 16 provides the conditional access information such as DES-encrypted transport streams 17 to a TD (transport demultiplexer) 18 within a graphics processor 60. The DES-encrypted transport stream 17 is reduced to a video PES (packetized elementary stream). The consumer's set top box or digital television system receives the DES-encrypted transport stream.

20 As known in the art, the TD 18 allows the graphics processor 60 to select an unencrypted compressed video stream from among those encoded in the DES-encrypted transport stream after the transport stream has been decrypted.

25 As shown, the TD outputs non-video information 27 that may be stored in the system memory. The unencrypted compressed video stream 25 is extremely valuable to illicit copiers, who can find a market in such video content. By simply copying the unencrypted compressed video stream from the TD 18 to the TD 18 onto a removable medium such as a CD-ROM, an illicit copier can produce a CD-ROM that can be sold.

30

The TD differentiates between the type of data. If the data is a compressed video stream, it is not sent to the CPU. For example, the central processing unit 44 receives close captioning, electronic program guide information, and other information contained within the transport stream.

5

The TD 18 provides the unencrypted compressed video stream to the memory controller 32. The memory controller 32 stores the unencrypted compressed video stream 25 in video buffer 40 within the frame buffer 38. The memory controller 32 receives requests for a block of unencrypted compressed video stream data when the 10 MPEG2 decoder 26 is ready to process. The TD 18 requests from the memory controller 32 a block of unencrypted compressed video stream stored in the video buffer 40. The MPEG-2 decoder 26 allows full-frame MPEG-2 images to be generated from the unencrypted compressed video stream. Specifically, the MPEG2 decoder 26 removes all of the headers from the packets, expands the unencrypted compressed video stream to 15 unencrypted uncompressed video picture and sends the unencrypted uncompressed video picture to the memory controller 32. The memory controller 32 stores the unencrypted uncompressed video pictures in the picture buffer 41 (i.e., display buffer) within the frame buffer 38.

20

The memory controller 32 receives requests for a line from the uncompressed video picture stored in the picture buffer 41 when the display engine 36 is ready to process the next presentation picture. The display engine 36 processes the unencrypted uncompressed video pictures for presentation to the monitor port, as known in the art.

25

As known in the art, the HBIU (Host Bus Interface Unit) 42 interfaces with the host CPU 44 and is used to allow, among other things, the host CPU 44 to access the frame buffer. Also, as is known, the 3D-processor 24 can move data within the frame buffer 38 by copying blocks of memory containing data into other blocks of memory that can receive data called a bit blit. For example, a user may execute a graphics program on 30 the central processing unit 44, and may indicate that the user wishes to drag a figure or stretch a figure. Accordingly, the 3D-processor 24 moves the data pertaining to the

figure from a first block of memory associated with the figure's original position and size to a second block of memory associated with the figure's new position and size.

In addition to providing the unencrypted uncompressed video stream via the
5 HBIU 42 to the memory controller 32, the HBIU 42 also permits the graphics processor
60 to operate with other devices over a user accessible bus 48 such as a PCI bus. The bus
48 may be a 33-MHz bus that couples the HBIU 42 of the graphics processor 60 to a
northbridge 46 or other PCI-compatible bus bridge, or any other suitable bus. The
northbridge 46 couples the central processing unit 44 to the PCI bus 48 and to system
10 memory 50. Other devices within the digital television system, such as the central
processing unit 44, may access resources within the graphics processor 60, and devices
within the graphics processor 60 may access other resources within the digital television
system, via the HBIU 42. Similarly, the graphics processor may access system resources
such as a system memory 50 via the PCI bus 48 and the northbridge 46.

15 System memory 50, such as SDRAM, is also available to the central processing
unit 44 via the northbridge 46. The graphics processor 60 therefore has three locations at
which an unscrupulous person seeking to produce an illicit copy might strike. One such
location is the input port, at which the graphics processor 60 receives data from the POD
20 module 16. However, as stated previously, the POD provides data that is encrypted using
a DES algorithm in ECB mode. Because the transport streams are encrypted,
intercepting the transport streams at this point does not allow an illicit copier to obtain a
marketable version of the video streams. Another location is the bus port, at which the
graphics processor 60 (via the HBIU 42) exchanges data and control information with the
25 PCI bus 48. A third location is the monitor port, at which the 3D-processor 24 and the
display engine 36 provide data to the monitor. Another location is the interface to the
external RAM.

At the second location, an unscrupulous person seeking to produce an illicit copy
30 may seek to copy the data in real-time, as it is provided from the HBIU 42 to the frame
buffer 38 via, among other elements, the HBIU 42. Because the HBIU 42 is coupled to

the PCI bus 48, it may be possible to intercept and copy the data passing through the HBIU 42 and copy the data onto another device coupled to the PCI bus 48. Although the graphics processor 60 is coupled to the PCI bus 48, copying the unencrypted uncompressed video stream via the HBIU 42 and the PCI bus 48 is extremely difficult.

5 Therefore is may not be necessary to encrypt this information.

For similar reasons, the unencrypted uncompressed video stream is not easily attainable at the third location (i.e., the monitor port), at least not in real time. The data from the graphics processor 60 to the monitor also has an extremely high data rate.

10 Moreover this information is typically protected through other mechanisms such as timing alterations (Macrovision) or HDCP based approach.

Since copying the data in real time is prohibitive, the unscrupulous person attempting to produce an illicit copy of the data may attempt to copy the data directly 15 from the frame buffer 38. This is possible since the frame buffer 38 is accessible to processes executing on the central processing unit 44. Moreover, the frame buffer 38 itself is amenable to having data moved from one location to another, as described above with respect to operations performed by the 3D-processor 24. Therefore, a software application could be used to obtain the data.

20 FIG. 2 shows a block diagram of a portion of a system in accordance with one embodiment of the present invention. It will be recognized that although shown as interfacing with a POD based system, the disclosed method and apparatus can be used with any encrypted data in any suitable system or arrangement. An 25 encryption/decryption module 202 is located between the memory controller 32 and in this example, the local (e.g., off chip or on-chip) frame buffer memory 38. A frame buffer stores information, including but not limited to compressed video, uncompressed video frames, graphics elements from a rendering engine, and frames for display. The encryption/decryption module 102 selectively encrypts at least some of the data passing 30 through the encryption/decryption module 102 en route to the local frame buffer memory 38 to provide encrypted data, and then stores the encrypted data in the local frame buffer

memory 38. Little or no unencrypted data corresponding to the data to be protected is stored in the frame buffer 38. The encryption module 102 also decrypts the encrypted data from the frame buffer 38 and provides decrypted data from the frame buffer 38 to the memory control 32.

5

The encryption/decryption module 202 operates, in one embodiment, using a DES encryption/decryption scheme. If desired, the encryption module 202 may operate using a public key/private key cryptographic operation, conditional access algorithm, or any other suitable cryptographic technique.

10

In accordance with one embodiment of the present invention, when any memory access client (e.g., the TD 18 or the CPU 44) attempts to pass (write) data to the local frame buffer 38, the encryption/decryption module 202 examines the address to which the data is being written. If the address indicates that the data is to be protected (i.e., falls within a defined address range), then the encryption module 102 encrypts the data to produce encrypted data, and then writes the encrypted data to the frame buffer 38. If desired, the encryption module 202 may also encrypt other data as well as producing additional encrypted data (not part of the transport stream) and write the additional encrypted data to the frame buffer 38 on an as-needed basis.

15

Alternatively, the encrypt/decryption module 202 may be incorporated as part of the TD 18 and encryption may be performed on a per stream basis based on configuration bits in the stream. For example, if a stream contains copy protected data, this stream is encrypted. Also, if desired, memory access may be granted or denied based upon the PID number (i.e., the packet identification number) that describes each packet. The PID of a received packet may be used in lieu of the address of the attempted access to grant or deny access.

20

Accordingly, even if an illicit copier managed to copy or move the data residing within the encrypted memory space to another (external) device such as a writable CD-ROM, Zip drive, hard drive, or other storage device, the data would be of little or no use

25

to the illicit copier. Only by decrypting the data using the appropriate keys could the illicit copier gain access to the content.

FIG. 3 shows a block diagram of a portion of a system, in accordance with yet another embodiment of the present invention. As shown in FIG. 3, the memory controller 32 includes a memory address protection module 304. The memory address protection module 304 contains or has access to at least one start access address register 305 and an end access address register 307 that identify a secure region within a non-local (or local) frame buffer 38. The start access address register 305 contains an address (or index thereto) that identifies a start boundary of the secure region of the video memory. Similarly, the end access address register 307 includes the end address of a contiguous register space within the non-local frame buffer 38 that is used as a FIFO, such as a video buffer 40.

The encryption/decryption module is shown as part of the memory access protection module may included as part of any suitable block. However, encryption need not be used and the secure region need not contain encrypted data since only specified clients are allowed to access the secure region. However, as described below, both address access limitation techniques and encryption techniques will be described. In accordance with one embodiment of the present invention, the graphics processor 60 contains both the encryption module 202 (FIG. 2) and the memory address protection module 304. Encryption of the frame buffer contents may be encrypted based on for example whether an address in within a secure region, whether the address is marked by an accessing client, on a per stream basis or any other suitable criteria.

If desired, the encrypted portion of the memory space may be in a contiguous region within the address space of the frame buffer 38. In other words, all addresses between a first threshold address and a second threshold address are directed to the encrypted memory space, and data written to the encrypted memory space is encrypted. Similarly, if desired, the encrypted portion of the memory space may be in a discontiguous region within the address space of the frame buffer 38. In other words, the

encrypted portion may be defined between pairs of threshold addresses, and all addresses between a first threshold address of each pair of threshold addresses and a second threshold address of each pair of threshold addresses are directed to the encrypted memory space, and data written to the encrypted memory space is encrypted.

5

In the example of FIG. 3, two access address registers 305 and 307 are provided, i.e. a first address register and a second address register. Each of the two access address registers 305 and 307 may contain an address within the video memory 40. When each of the access address registers 305 and 307 contains an address, the two address registers 10 305 and 307 define a bounded region within the video memory that cannot be accessed by the central processing unit 44. The memory address protection module 304 prevents the central processing unit, and any other bus masters on the PCI bus 48 or attempts to access the video memory via the HBIU 42, from reading data stored in the secure region.

15

If desired, a plurality of comparators and comparison logic may be used as part of the memory address protection module 304. Each of the comparators is coupled to a distinct access address register containing a pointer, and is operative to compare the pointer to an address of an attempted access. The comparison logic is operative to determine, based on output from the comparators, whether the address of an attempted 20 access is within a protected region of the video memory.

20

Alternatively, if desired, only one access address register (305 or 307) is provided. The access address register may contain an address within the video memory or any portion of frame buffer. When the access address register contains an address, the 25 address register containing memory location define a bounded region within the video memory that cannot be accessed by the central processing unit. For example, all memory locations beyond (or above) the threshold address in the access address register fall within the bounded region within the video memory that cannot be accessed by the central processing unit. The memory address protection module 304 prevents the central 30 processing unit, and any other bus masters on the PCI bus 48 or attempts to access the video memory via the HBIU 42, from reading data stored in the secure region. In

operation, the memory controller 32 passes substituted data (“bad” data) back to the CPU to complete the access cycle. For example, if a memory request by the CPU for data is in the secure region, the memory controller reads data from a nonsecure portion instead of the secure portion.

5

In another embodiment, multiple bounded regions may be provided. Specifically, multiple pairs of access address registers are provided. Each of the access address registers of any pair may contain an address within the video memory. When each of the address registers of any pair contains an address, the two access address registers 305 and 10 307 define a bounded region within the video memory that cannot be accessed by the central processing unit. The memory address protection module 304 prevents the central processing unit, and any other bus masters on the PCI bus 48 or attempting to access the video memory via the HBIU 42, from reading data stored in the secure region.

15

The graphics processor 60 is configurable as a secure chip or as an unsecure chip. Such configuration cannot easily be altered once the chip has been manufactured. When configured as a secure chip, the access address registers 305 and 307 are wire-bonded to be writable only when empty. The configuration as whether a secure chip or an unsecure chip is determined by a single secure chip designation bit 308 (or multiple bits if desired) 20 residing within the graphics processor 60 itself. The single bit 308 may be set or cleared by either the manufacturer of the chip or an OEM (original equipment manufacturer) manufacturing a system containing the chip. In accordance with one embodiment of the present invention, the single bit 308 is a fusible (or antifusible) connection to either power or ground. If desired, the single bit 308 may be read from a ROM residing on the 25 graphics processor 60.

The single bit 308 is such that tampering with the single bit 308 cannot reduce the security of the graphics processor 60. For example, the graphics processor 60 may be manufactured as an unsecure chip and may be converted to a secure chip by fusing or 30 antifusing a connection to either power or to ground. Similarly, the graphics processor 60 may be manufactured such that the single bit is inaccessible to external tampering.

Accordingly, tampering cannot convert the graphics processor 60 from a secure chip to an unsecure chip.

A non-reversible mechanism is used to convert the graphics processor 60 to a 5 secure chip before shipping. However for debugging purposes, the chip is configured in an unsecure mode. To configure the graphics processor 60 as an unsecure chip, the single bit is set to an “1” or “0” via simple circuit such as a resistor and fuse configuration. A pin (bit) may be connected to power via a resistor, and to ground via a fuse. The graphics processor 60 may then be converted to a secure chip by fusing the 10 fuse. If desired, single bit may be connected to power via an antifuse, and to ground via a resistor. The graphics processor 60 may then be converted to a secure chip by antifusing the antifuse. Because fusing and antifusing are difficult for the typical end user to 15 perform, the graphics processor 60 is not easily converted by the end user from a secure chip to an unsecure chip, since the single bit is a fusible (or antifusible) connection to either power or ground.

In addition, the graphics processor 60 also includes a reversible process for 20 turning on and off the encryption/ access register modes. Such a graphics processor 60 contains suitable logic (not shown) such as an AND gate, the output of which disables the encryption module 202 or the memory address protection module 304 via an enable signal, i.e. the components that permit or deny access to an unencrypted version of the data that is to be protected to configure the chip as an unsecure chip. The input being accessible via a pin or internal register to toggle between the secure and non-secure mode so that testing of the chip in both modes can be accomplished.

25 If desired, the single bit may reside in software implemented within a ROM residing on the graphics processor 60. Firmware (basic input output system) or other operation determines whether the chip is a secure chip or an unsecure chip. In accordance with one embodiment of the present invention, the single bit may be set or cleared by 30 either the manufacturer of the chip or an OEM manufacturing a system containing the chip. If desired, the single bit may be read from a ROM residing on the graphics

processor 60. The ROM may be flash memory that may be written at any time by the manufacturer of the chip or by an OEM, but is not easily re-written by an end user.

During initial configuration (usually after power-up or system reset), the CPU 44 determines whether the graphics processor 60 is configured to be secure. This may be done by reading a configuration register containing the secure chip designation bit. If the graphics processor 60 is secure, the CPU 44 proceeds to write the access address registers to define the "secure" area(s) in the video memory. This is done while the CPU 44 is executing initialization code that may be part of the BIOS, or operating system initialization code. This initialization code is considered safe, since it is provided by the manufacturer or OEM and is stored in system ROM or graphics processor ROM, and the manufacturer or OEM has taken steps to insure that this code is not easily modified by users.

The access address registers 305, 307 in the memory access protection module 304 can be written only once. All subsequent writes to these registers will be ignored. The only way to enable writing to these registers again is to initiate a hardware reset of the graphics processor 60. Therefore, once the secure area(s) has been set up by the initialization code, a rogue SW program will not be able to gain access to the secure area of video memory by rewriting the access address registers.

FIG. 4 shows a flowchart of a process of accessing data on a graphics processor, assuming the chip is configured as a secure chip. The process begins at step 250 and proceeds to step 252. At step 252, an address of an attempted access is received, for example, by the memory controller 32 containing the address protection module 304 from a memory reading client. At step 253, the process includes determining, such as by the memory access protection module, whether the graphics processor is configured for secure operation as indicated for example by the secure chip designation bit. If the graphics processor 60 is not configured as a secure chip, the process is terminated as shown in block 270 and access is permitted. However, if the graphics processor 60 is configured as a secure chip, the process continues to block 255 where the address of the

attempted access is compared with the contents of the access registers to determine whether the attempted access is to a protected address or address range. If so, the process continues to block 256. Otherwise the process continues to block 270.

5 At step 256, the memory reading client that is attempting access is identified to determine whether it is an authorized reading client or an unauthorized reading client. This is done by reading the client access privilege register (CAPR) when a new request is made on a memory access port to determine whether the reading client is designated as an approved frame buffer reading client. The reading client may be, for example, the bus 10 master, a graphics processor, central processing unit or other circuit that has attempted to access the video memory by providing the address.

Step 256 need not determine the reading client with any specificity, but does 15 determine a permission associated with the client. The permission is either “permit” or “deny” based on the content of the client access privilege register 309. For example if the register 309 is fused or programmed to indicate that the video decoder 26 reading client has access to the range of secure addresses, the memory controller allows access to the address range if a request is received via its decoder port. Similarly, the register 309 may have a deny indication for the HBIU 42, the 3D processor 34 and the display engine 20 36. It will be recognized that if the client access privilege register (CAPR) is used, the secure chip designation bit is not necessary.

Alternatively, if desired, access may be granted or denied based upon the PID 25 number (i.e., the packet identification number) that describes each packet. The PID of a received packet may be used in lieu of the address of the attempted access to grant or deny access.

If the memory address protection module determines that the permission is not 30 “permit,” then the process proceeds to step 272 and terminates such that substituted data (e.g., data other than from the secure region) is sent back to the reading client and nothing

is written (e.g., access is denied) if the request is a write request. If it is determined that the permission is “permit,” then the process proceeds to step 259.

At step 259, if the memory access protection module is configured to 5 encrypt/decrypt data, the process continues to step 260 where encryption is performed by the encryption/decryption module 202 if the access is a write access, and decryption is performed if the access is a read access. The process then proceeds to step 270 and terminates such that access is permitted.

10 In accordance with another embodiment of the present invention, at step 272 the process indicates to the originator of the attempted access that the attempted access is denied. In other words, the originator receives an error message indicating that the attempted access has failed.

15 If desired, instead of (or in addition to) providing an error message at step 272, the process provides a null value or a predetermined value. The predetermined value is, for example, zero. The predetermined value may be obtained from a register, or may be “hard-wired.” Alternatively, if desired, instead of (or in addition to) providing an error message, the process redirects the attempted access to a predetermined memory location. 20 The predetermined memory location is, for example, an unsecure location in the video memory.

As described above, hardware and/or software may be used to prevent bus masters coupled to the graphics processor via a user from accessing portions of the video 25 memory while permitting access to other portions. The location of the HBIU 42(i.e., whether the HBIU with bus master is located on-chip or off-chip), the configuration of the graphics processor itself, the address of the attempted access, and the type of data being accessed can be relevant in determining whether access is permitted or denied. Accordingly, bus masters coupled to the graphics processor via the PCI bus 48 are denied 30 access to the unencrypted compressed video, even though the unencrypted compressed video is stored on the graphics processor, and even though the bus masters coupled to the

graphics processor via the PCI bus 48 can access other portions of the video memory. An encryption module may be desirable where the video memory is not on-chip with a graphics engine or DES descrambler. An address-based access control scheme (with or without encryption) may be desirable when the frame buffer is local.

5

Where only encryption/decryption is used instead of access registers, the memory controller encrypts or decrypts data if the accessing client is indicated as an approved client. Where only the access registers are used, the address being accessed determines whether access is allowed.

10

It should be understood that the implementation of other variations and modifications of the invention in its various aspects will be apparent to those of ordinary skill in the art, and that the invention is not limited by the specific embodiments described. For example, the graphics processor may be a collection of graphics chips residing on multiple graphics cards, sharing a common configuration (i.e., either secure or unsecure) and sharing comparator logic. The graphics chip may be a graphics processor within a larger system on a chip configuration. It is therefore contemplated to cover by the present invention, any and all modifications, variations, or equivalents that fall within the spirit and scope of the basic underlying principles disclosed and claimed herein.

2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 20100 20101 20102 20103 20104 20105 20106 20107 20108 20109 20110 20111 20112 20113 20114 20115 20116 20117 20118 20119 20120 20121 20122 20123 20124 20125 20126 20127 20128 20129 20130 20131 20132 20133 20134 20135 20136 20137 20138 20139 20140 20141 20142 20143 20144 20145 20146 20147 20148 20149 20150 20151 20152 20153 20154 20155 20156 20157 20158 20159 20160 20161 20162 20163 20164 20165 20166 20167 20168 20169 20170 20171 20172 20173 20174 20175 20176 20177 20178 20179 20180 20181 20182 20183 20184 20185 20186 20187 20188 20189 20190 20191 20192 20193 20194 20195 20196 20197 20198 20199 20200 20201 20202 20203 20204 20205 20206 20207 20208 20209 202010 202011 202012 202013 202014 202015 202016 202017 202018 202019 202020 202021 202022 202023 202024 202025 202026 202027 202028 202029 202030 202031 202032 202033 202034 202035 202036 202037 202038 202039 202040 202041 202042 202043 202044 202045 202046 202047 202048 202049 202050 202051 202052 202053 202054 202055 202056 202057 202058 202059 202060 202061 202062 202063 202064 202065 202066 202067 202068 202069 202070 202071 202072 202073 202074 202075 202076 202077 202078 202079 202080 202081 202082 202083 202084 202085 202086 202087 202088 202089 202090 202091 202092 202093 202094 202095 202096 202097 202098 202099 2020100 2020101 2020102 2020103 2020104 2020105 2020106 2020107 2020108 2020109 2020110 2020111 2020112 2020113 2020114 2020115 2020116 2020117 2020118 2020119 2020120 2020121 2020122 2020123 2020124 2020125 2020126 2020127 2020128 2020129 2020130 2020131 2020132 2020133 2020134 2020135 2020136 2020137 2020138 2020139 2020140 2020141 2020142 2020143 2020144 2020145 2020146 2020147 2020148 2020149 2020150 2020151 2020152 2020153 2020154 2020155 2020156 2020157 2020158 2020159 2020160 2020161 2020162 2020163 2020164 2020165 2020166 2020167 2020168 2020169 2020170 2020171 2020172 2020173 2020174 2020175 2020176 2020177 2020178 2020179 2020180 2020181 2020182 2020183 2020184 2020185 2020186 2020187 2020188 2020189 2020190 2020191 2020192 2020193 2020194 2020195 2020196 2020197 2020198 2020199 2020200 2020201 2020202 2020203 2020204 2020205 2020206 2020207 2020208 2020209 2020210 2020211 2020212 2020213 2020214 2020215 2020216 2020217 2020218 2020219 2020220 2020221 2020222 2020223 2020224 2020225 2020226 2020227 2020228 2020229 2020230 2020231 2020232 2020233 2020234 2020235 2020236 2020237 2020238 2020239 2020240 2020241 2020242 2020243 2020244 2020245 2020246 2020247 2020248 2020249 2020250 2020251 2020252 2020253 2020254 2020255 2020256 2020257 2020258 2020259 2020260 2020261 2020262 2020263 2020264 2020265 2020266 2020267 2020268 2020269 2020270 2020271 2020272 2020273 2020274 2020275 2020276 2020277 2020278 2020279 2020280 2020281 2020282 2020283 2020284 2020285 2020286 2020287 2020288 2020289 2020290 2020291 2020292 2020293 2020294 2020295 2020296 2020297 2020298 2020299 2020300 2020301 2020302 2020303 2020304 2020305 2020306 2020307 2020308 2020309 2020310 2020311 2020312 2020313 2020314 2020315 2020316 2020317 2020318 2020319 2020320 2020321 2020322 2020323 2020324 2020325 2020326 2020327 2020328 2020329 2020330 2020331 2020332 2020333 2020334 2020335 2020336 2020337 2020338 2020339 2020340 2020341 2020342 2020343 2020344 2020345 2020346 2020347 2020348 2020349 2020350 2020351 2020352 2020353 2020354 2020355 2020356 2020357 2020358 2020359 2020360 2020361 2020362 2020363 2020364 2020365 2020366 2020367 2020368 2020369 2020370 2020371 2020372 2020373 2020374 2020375 2020376 2020377 2020378 2020379 2020380 2020381 2020382 2020383 2020384 2020385 2020386 2020387 2020388 2020389 2020390 2020391 2020392 2020393 2020394 2020395 2020396 2020397 2020398 2020399 2020400 2020401 2020402 2020403 2020404 2020405 2020406 2020407 2020408 2020409 2020410 2020411 2020412 2020413 2020414 2020415 2020416 2020417 2020418 2020419 2020420 2020421 2020422 2020423 2020424 2020425 2020426 2020427 2020428 2020429 2020430 2020431 2020432 2020433 2020434 2020435 2020436 2020437 2020438 2020439 2020440 2020441 2020442 2020443 2020444 2020445 2020446 2020447 2020448 2020449 2020450 2020451 2020452 2020453 2020454 2020455 2020456 2020457 2020458 2020459 2020460 2020461 2020462 2020463 2020464 2020465 2020466 2020467 2020468 2020469 2020470 2020471 2020472 2020473 2020474 2020475 2020476 2020477 2020478 2020479 2020480 2020481 2020482 2020483 2020484 2020485 2020486 2020487 2020488 2020489 2020490 2020491 2020492 2020493 2020494 2020495 2020496 2020497 2020498 2020499 2020500 2020501 2020502 2020503 2020504 2020505 2020506 2020507 2020508 2020509 2020510 2020511 2020512 2020513 2020514 2020515 2020516 2020517 2020518 2020519 2020520 2020521 2020522 2020523 2020524 2020525 2020526 2020527 2020528 2020529 2020530 2020531 2020532 2020533 2020534 2020535 2020536 2020537 2020538 2020539 2020540 2020541 2020542 2020543 2020544 2020545 2020546 2020547 2020548 2020549 2020550 2020551 2020552 2020553 2020554 2020555 2020556 2020557 2020558 2020559 2020560 2020561 2020562 2020563 2020564 2020565 2020566 2020567 2020568 2020569 2020570 2020571 2020572 2020573 2020574 2020575 2020576 2020577 2020578 2020579 2020580 2020581 2020582 2020583 2020584 2020585 2020586 2020587 2020588 2020589 2020590 2020591 2020592 2020593 2020594 2020595 2020596 2020597 2020598 2020599 2020600 2020601 2020602 2020603 2020604 2020605 2020606 2020607 2020608 2020609 2020610 2020611 2020612 2020613 2020614 2020615 2020616 2020617 2020618 2020619 2020620 2020621 2020622 2020623 2020624 2020625 2020626 2020627 2020628 2020629 2020630 2020631 2020632 2020633 2020634 2020635 2020636 2020637 2020638 2020639 2020640 2020641 2020642 2020643 2020644 2020645 2020646 2020647 2020648 2020649 2020650 2020651 2020652 2020653 2020654 2020655 2020656 2020657 2020658 2020659 2020660 2020661 2020662 2020663 2020664 2020665 2020666 2020667 2020668 2020669 2020670 2020671 2020672 2020673 2020674 2020675 2020676 2020677 2020678 2020679 2020680 2020681 2020682 2020683 2020684 2020685 2020686 2020687 2020688 2020689 2020690 2020691 2020692 2020693 2020694 2020695 2020696 2020697 2020698 2020699 2020700 2020701 2020702 2020703 2020704 2020705 2020706 2020707 2020708 2020709 2020710 2020711 2020712 2020713 2020714 2020715 2020716 2020717 2020718 2020719 2020720 2020721 2020722 2020723 2020724 2020725 2020726 2020727 2020728 2020729 2020730 2020731 2020732 2020733 2020734 2020735 2020736 2020737 2020738 2020739 2020740 2020741 2020742 2020743 2020744 2020745 2020746 2020747 2020748 2020749 2020750 2020751 2020752 2020753 2020754 2020755 2020756 2020757 2020758 2020759 2020760 2020761 2020762 2020763 2020764 2020765 2020766 2020767 2020768 2020769 2020770 2020771 2020772 2020773 2020774 2020775 2020776 2020777 2020778 2020779 2020780 2020781 2020782 2020783 2020784 2020785 2020786 2020787 2020788 2020789 2020790 2020791 2020792 2020793 2020794 2020795 2020796 2020797 2020798 2020799 2020800 2020801 2020802 2020803 2020804 2020805 2020806 2020807 2020808 2020809 2020810 2020811 2020812 2020813 2020814 2020815 2020816 2020817 2020818 2020819 2020820 2020821 2020822 2020823 2020824 2020825 2020826 2020827 2020828 2020829 2020830 2020831 2020832 2020833 2020834 2020835 2020836 2020837 2020838 2020839 2020840 2020841 2020842 2020843 2020844 2020845 2020846 2020847 2020848 2020849 2020850 2020851 2020852 2020853 2020854 2020855 2020856 2020857 2020858 2020859 2020860 2020861 2020862 2020863 2020864 2020865 2020866 2020867 2020868 2020869 2020870 2020871 2020872 2020873 2020874 2020875 2020876 2020877 2020878 2020879 2020880 2020881 2020882 2020883 2020884 2020885 2020886 2020887 2020888 2020889 2020890 2020891 2020892 2020893 2020894 2020895 2020896 2020897 2020898 2020899 2020900 2020901 2020902 2020903 2020904 2020905 2020906 2020907 2020908 2020909 2020910 2020911 2020912 2020913 2020914 2020915 2020916 2020917 2020918 2020919 2020920 2020921 2020922 2020923 2020924 2020925 2020926 2020927 2020928 2020929 2020930 2020931 2020932 2020933 2020934 2020935 2020936 2020937 2020938 2020939 2020940 2020941 2020942 2020943 2020944 2020945 2020946 2020947 2020948 2020949 2020950 2020951 2020952 2020953 2020954 2020955 2020956 2020957 2020958 2020959 2020960 2020961 2020962 2020963 2020964 2020965 2020966 2020967 2020968 2020969 2020970 2020971 2020972 2020973 2020974 2020975 2020976 2020977 2020978 2020979 2020980 2020981 2020982 2020983 2020984 2020985 2020986 2020987 2020988 2020989 2020990 2020991 2020992 2020993 2020994 2020995 2020996 2020997 2020998 2020999 20201000 20201001 20201002 20201003 20201004 20201005 20201006 20201007 20201008 20201009 202010010 202010011 202010012 202010013 202010014 202010015 202010016 202010017 202010018 202010019 202010020 202010021 202010022 202010023 202010024 202010025 202010026 202010027 202010028 202010029 202010030 202010031 202010032 202010033 202010034 202010035 202010036 202010037 202010038 202010039 202010040 202010041 202010042 202010043 202010044 202010045 202010046 202010047 202010048 202010049 202010050 202010051 202010052 202010053 202010054 202010055 202010056 202010057 202010058 202010059 202010060 202010061 202010062 202010063 202010064 202010065 202010066 202010067 202010068 202010069 202010070 202010071 202010072 202010073 202010074 202010075 202010076 202010077 202010078 202010079 202010080 202010081 202010082 202010083 202010084 202010085 202010086 202010087 202010088 202010089 202010090 202010091 202010092 202010093 202010094 202010095 202010096 202010097 202010098 202010099 2020100100 2020100101 2020100102 2020100103 2020100104 2020100105 2020100106 2020100107 2020100108 2020100109 2020100110 2020100111 2020100112 2020100113 2020100114 2020100115 2020100116 2020100117 2020100118 2020100119 2020100120 2020100121 2020100122 2020100123 2020100124 2020100125 2020100126 2020100127 2020100128 2020100129 2020100130 2020100131 2020100132 2020100133 2020100134 2020100135 2020100136 2020100137 2020100138 2020100139 2020100140 2020100141 2020100142 2020100143 2020100144 2020100145 2020100146 2020100147 2020100148 2020100149 2020100150 2020100151 2020100152 2020100153 2020100154 2020100155 2020100156 2020100157 2020100158 2020100159 2020100160 2020100161 2020100162 2020100163 2020100164 2020100165 2020100166 2020100167 2020100168 2020100169 2020100170 2020100171 2020100172 2020100173 2020100174 2020100175 2020100176 2020100177 2020100178 2020100179 2020100180 2020100181 2020100182 2020100183 20201001